Hong Zimeng

Security of Mobile Devices and Wi-Fi Networks

Bachelor's Thesis

Information Technology

May 2015

MAMK
University of Applied Sciences

DESCRIPTION

MAMK University of Applied Sciences	**Date of the bachelor's thesis** 28. 05. 2015
Author(s) Hong Zimeng	**Degree programme and option** Information Technology

Name of the bachelor's thesis

Security of Mobile Devices and Wi-Fi Networks

Abstract

Along with the progress of times and the development of science and technology, mobile devices have become more and more popular. At the same time, an increasing number of Wi-Fi networks are being built for the demand of mobile devices. Therefore, the security between mobile devices and Wi-Fi networks became a main object in the IT area. The purpose of the thesis is to analyze security threats and give relative advises for all the mobile device and Wi-Fi network users.

The thesis mainly talks about two types security issues. For individual mobile device users, the threats mainly come from the public Wi-Fi networks they are using to transmit important message or information. For enterprise Wi-Fi networks, the security focus on preventing organization from mobile devices attacks.

In order to reach the security object for individual mobile device users and enterprise Wi-Fi networks, the purpose of security technologies are from three dimensions: confidentiality, integrity and authentication. As an example of a secure communication method for mobile device users to encrypted data transmission I implement a clientless SSL based VPN connection between a mobile device and a firewall.

The thesis could be used as a security guide for mobile device users and Wi-Fi network organizations, helping them to prevent security from Internet attacks.

Subject headings, (keywords)

Security, Wi-Fi network, Mobile device,

Pages	**Language**	**URN**
41	English	

Remarks, notes on appendices

Tutor	**Bachelor's thesis employed by**
Matti Koivisto	Mikkeli University of Applied Science

CONTENTS

1. INTRODUCTION

Along with the progress of times and the development of science and technology, mobile devices have become more and more popular. They play an increasingly important role not only because of higher performance, but also because they are portable computing device. The Bring Your Own Device (BYOD) idea has been accepted by many people to be used their personal mobile devices and at work.

For mobile devices to connect to the Internet anytime anywhere they have wireless cards pre-installed. They can be connected to the Internet with cellular networks like 3G or 4G networks. In addition to that, a high bandwidth alternative Wi-Fi is gaining more attraction among mobile device users.

Wi-Fi, also named Wireless Fidelity, is based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. It offers a high transmission speed and effectively guarantees the network stability and reliability. In an open area the communication distance could be up to about 300 meters. In an office environment the communication distance is around 100 meters.

1.1. Purpose and Scope

In wired networks data is sent between two points connected by a network cable. Therefore, the data is not easily accessed by an unauthorized third-party. However, wireless networks broadcast data to every direction. On the other hand, listening and reading could happen in every permissive device. In other words, wireless networks provide more possibilities for unauthorized access, even for damage to electronic devices.

The purpose of this study is to analyze different security threats mobile devices face in the Wi-Fi environment. In this thesis the environment will be divided by scale into the enterprise Wi-Fi network security against mobile device attacks and the individual mobile devices against attacks from Wi-Fi networks.

In general, a mobile device is a small, handheld computing device. Smartphones and tablets are the most common mobile devices in our daily work and entertainment. Some mobile devices like a cell phone with minimal computing capability are excluded from the scope of mobile devices in this report. Because the security deployment of laptops is quite different

from that of smartphone and tablets, laptops are also excluded from the mobile devices that are discussed in this report.

According to the status of the recent mobile device market, the iOS and the Android operating system account for over 95% of the usage in total (IDC 2015). Therefore, the mobile devices mentioned in this thesis will focus on the iOS and the Android Operating System.

This thesis is based both on previous research, and the practical work done by me. The aim of the practice part is to implement mobile device user with a SSL based Virtual Private Network (VPN). Unlike WLAN security technologies such as WPA and WPA2, VPN provides end-to-end security between the mobile device and VPN firewall. Because there is large number of different type of mobile devices, the VPN will be implement using a clientless approach.

This work could be used as a security guide for wireless users to help them to prevent their electronic devices from Internet attacks.

1.2. Thesis Structure

This thesis has seven chapters. After the introduction, the second chapter introduces the operating system, application and network connections of mobile devices. The third chapter focuses on security technologies for wireless networks, which mainly includes encryption technology and authentication technology. The following two chapters discuss two different situations. Chapter 4 considers mobile devices' security issues under the Wi-Fi network, and Chapter 5 focuses on enterprise Wi-Fi network threats from mobile devices. My practical implementation of a secure VPN connection is reported in chapter 6. Finally, I summarize the results of my study in the last chapter.

2. OVERVIEW ON MOBILE DEVICES

In this chapter I mainly discuss the characteristics of mobile devices. As mentioned earlier, the current mobile device market is dominated by two operating systems: iOS and Android, which are also the only operating systems in my study. First of all, I present the general introduction to mobile operating systems. Next, I talk about the mobile apps, especially malicious apps. In addition to this, I would give some possible protection solutions. Finally, I introduce the different methods to connect to the wireless network.

2.1. Mobile Operating Systems

2.1.1. Android Operating System

The Android operating system is based on the Linux kernel and currently developed by Google. As the clear leader in the mobile operating system race, Android is famous as a ready-made, low-cost and customizable operating system for mobile devices. According to IDC Worldwide Quarterly Mobile Phone Tracker, Android still stay the leader proportion of mobile operating system market with a market share reaching to 81.5% in the year of 2014. (IDC 2015)

The Android system was original developed by Andy Rubin, and the original purpose of this system was to develop an advanced digital camera operating system. Soon, Android was transformed into an operating system for smart mobile devices. In the August of 2005 Google acquired the Android system. In November 2007, Google cooperated with 84 hardware manufacturers, software developers and telecommunications operators and founded Open Handset Alliance to co-develop and to improve the Android system. Finally, Google depended on a free open-source Apache license, and released the source code of Android. In the next period of time the Android operating system gradually extended to the area of mobile devices like smartphones and tablets. (Gizmodo 2007)

2.1.2. iOS

The second strong leader of mobile operating systems, iOS was developed by Apple Company and distributed exclusively for Apple hardware. Similar to Apple's Mac OS X computer operating system, iOS belongs to the class of the commercial Unix operating system.

The iPhone operating system was first unveiled with iPhone on January 9, 2007, and released in June of the same year. Soon afterwards, iOS extended to support other Apple mobile devices such as iPod Touch, and iPad. Since iPad, iPhone and iPod Touch use the iPhone OS, Apple Company renamed this system into iOS and announced it at the WWDC Assembly of 2010. (Wikipedia, 2015)

By the end of 2012 iOS accounted for 21% and 43.6% of the smartphone and tablet market respectively (IDC 2013). As of February 2015, StatCounter Global Stats indicate that iOS was used on 23.18% of smartphones and 66.25% of tablets (StatCounter Global, 2015).

2.2. Mobile Apps

A mobile app is a computer program designed based on the operating system to run on mobile devices. The term “app” is short for the term “application software”. Until now, both iOS and Android can offer millions apps. The number of available apps in the Google Play Store surpassed 1 million apps in July 2013 and was most recently placed at 1.4 million apps in February 2015 (Statista, 2015). Apple Company says in January 2015: “There are now 1.4 million apps (725,000 native iPad apps) in the Apple App Store. Developers have now earned $25bn from apps in the Apple App Store - $10bn in 2014, with $500m spent on apps in January alone.”

2.2.1. Malicious App

Since the popularity of mobile apps has continued to increase, more and more workers in the IT field rely on developing mobile apps. Therefore, there is a wide variety of potential risks for mobile devices created by malicious developers. As an open-source operating system, Android attracts new developers continuously. On one hand, developers innovate new functions for apps. On the other hand, this provides hackers with an opportunity to hide vulnerabilities inside a malicious app, which is defined by its malicious intent, acting against the requirements of mobile device users. Malicious apps introduced through the Google Play store have increased by 388% between 2011 and 2013 (RiskIQ 2014). As one type of virus, malicious apps could disrupt mobile device operation, gather sensitive information and gain access to private operating systems.

Even though iOS established strict regulations for developers to release product in the Apple digital distribution platform, and users can only download app directly from Apple App Store.

The illegal third-party apps can still run on the iOS through Cydia Utilities. They could be installed on the Apple mobile devices after jailbreak. Although most iOS users know this possible danger, some of them prefer to jailbreak so that their Apple devices can pass Apple's purchase mechanism for installing the App Store's native applications. However, these apps are facing destruction with the iOS updates that could patch the un-patched jailbreak exploits.

In some cases apps that contained Trojans were hidden in the pirated versions of legitimate apps. This exploit allowed hackers to steal information such as phone model, user ID, IMEI (International Mobile Station Equipment Identity) and IMSI (International Mobile Subscriber Identity) numbers and the service provider. In many cases the exploit also installed a backdoor that allowed hackers to download more code to this infected device.

2.2.2. Official App Store

Generally speaking, the most reliable way to install apps on Android and iOS is through their native app stores like Google Play store and Apple App store provide the entire available app with official secure authentication.

The Google inspection system created Google Bouncer that is an in-house automated antivirus system to delete malicious apps uploaded onto their marketplace. Bouncer could not only prevent repeat-offender developers, but could also check anomalies in uploaded apps. Bouncer has been credited with lowering the number of "potentially" malicious downloads in the Android Market by 40 per cent between the first and second quarters of 2011. (Kaplan 2012)

Google Play displays all the permissions that an app requires before being installed, so that users can decide whether to install this app or not after reviewing its permissions. These app permissions include: accessing the Internet, making phone calls, sending SMS messages, reading from and writing to the installed memory card, accessing a user's address book data, visiting your locations, etc. Figure 1 shows the permissions in Google Play store for installing Facebook.

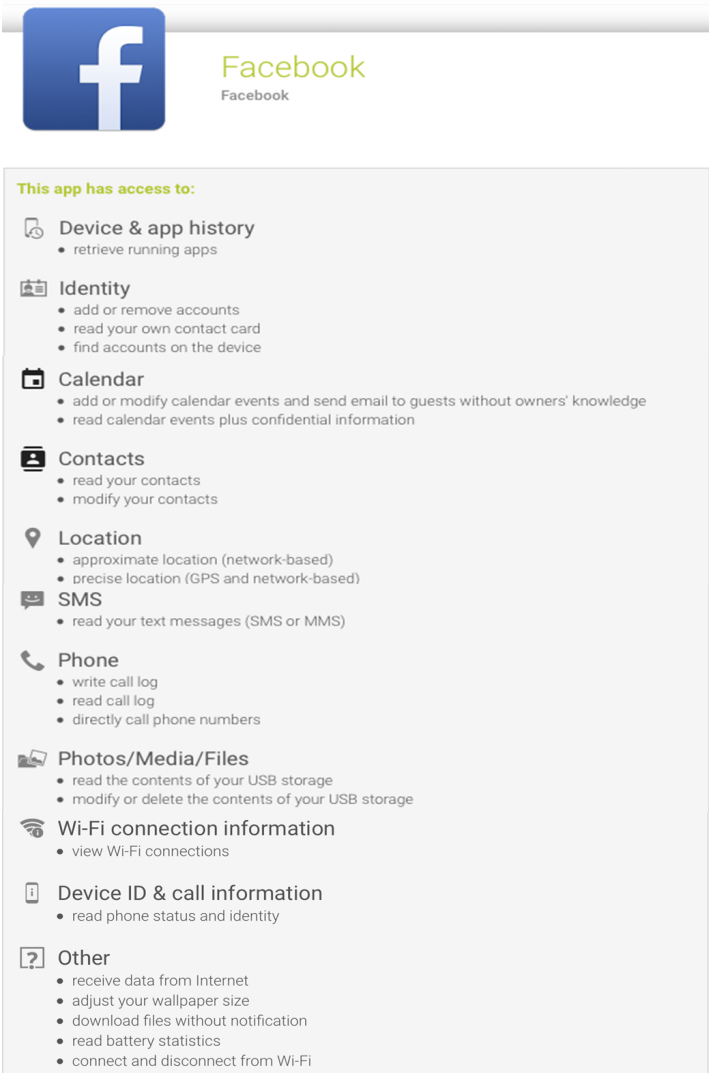

FIGURE 1. Permissions of Facebook app in Google Play

In contrast, iOS has extremely low user rights. As the only source of third-party apps, Apple App store has a rigorous examination for all third-party apps. In addition to that, Apple Company strictly limited the developer's permissions. Therefore, without jailbreak, there is no chance for malicious apps to appear in iOS, while is a closed system with the UNIX kernel and sandbox mechanism.

2.3. Network Connections of Mobile Devices

Mobile devices access to the Internet mainly depends on their wireless network interface connection. Commonly, digital cellular networks and wireless local area networks are the two types of network connection for mobile devices owners in their daily life.

2.3.1. Digital Cellular Network Connection

There is a number of different digital cellular technologies, including Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), cdmaOne, CDMA2000, Evolution-Data Optimized (EV-DO), Enhanced Data Rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), Digital Enhanced Cordless Telecommunications (DECT), Digital AMPS (IS-136/TDMA), and Integrated Digital Enhanced Network (iDEN). Major telecommunications providers have deployed data cellular networks over most of the inhabited land area of the Earth. This allows mobile devices to be connected to this cellular network directly, which ensures the safety of the data transmission channel.

Both the iOS and Android mobile device can open or close the cellular network easily. The left of Figure 2 shows that before the Android mobile device connects to the cellular network, the ‘mobile data’ icon is dark. After clicking the icon, on the right in Figure 2 we can see that the icon is light, which indicates this mobile device could access Internet successfully by connecting the cellular network.

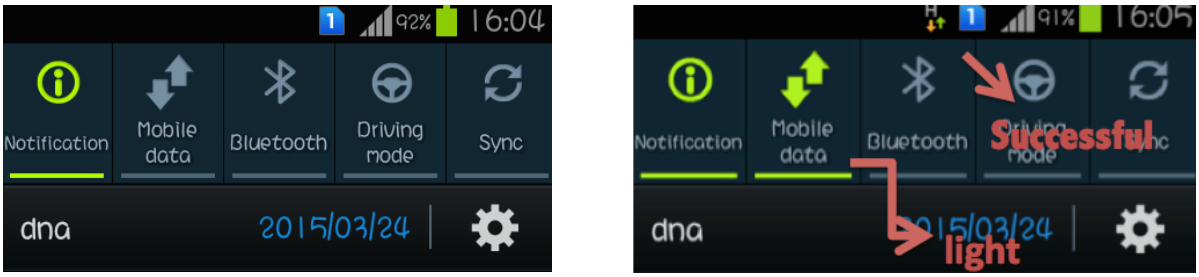

FIGURE 2. Mobile devices connect to cellular network

2.3.2. Wi-Fi Network Connection

The other way for mobile devices to connect to the Internet is through a wireless local area network, which is also named Wi-Fi. In order to access the Internet by connecting to the Wi-Fi network, we need to find first the ‘WLAN’ in the settings of the mobile device for both Android and iOS. Figure 3 shows the Android system on the left position and the iOS on the right.

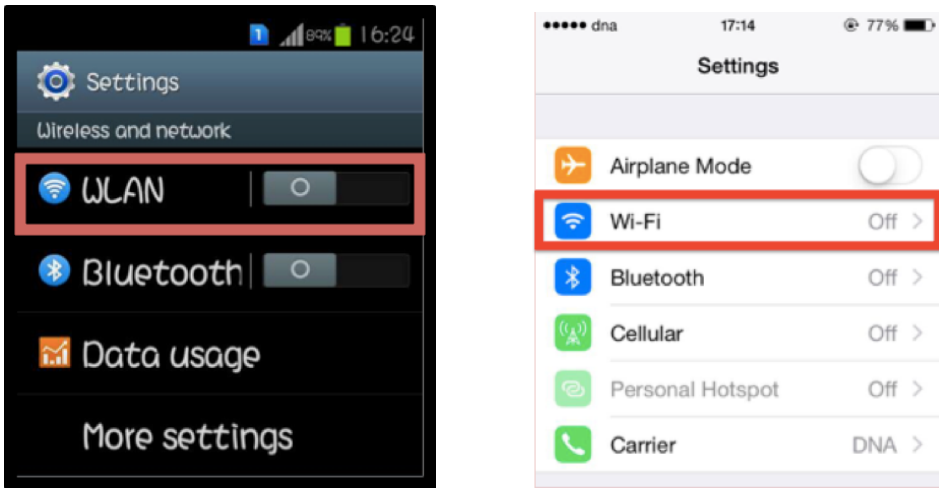

FIGURE 3. Wi-Fi connection in these mobile device's settings

Next, we need to open the 'WLAN' icon of Android, which is called 'Wi-Fi' in iOS. Hence, we can see all the available Wi-Fi networks in the range of your position with signal strength and whether there us need for a password or not. If a user has turned on the automatic Wi-Fi connection, the mobile device can be automatically connected Internet access without a password.

In general, the free open one will be connected automatically to the Internet than those with passwords (shown in Figure 4).

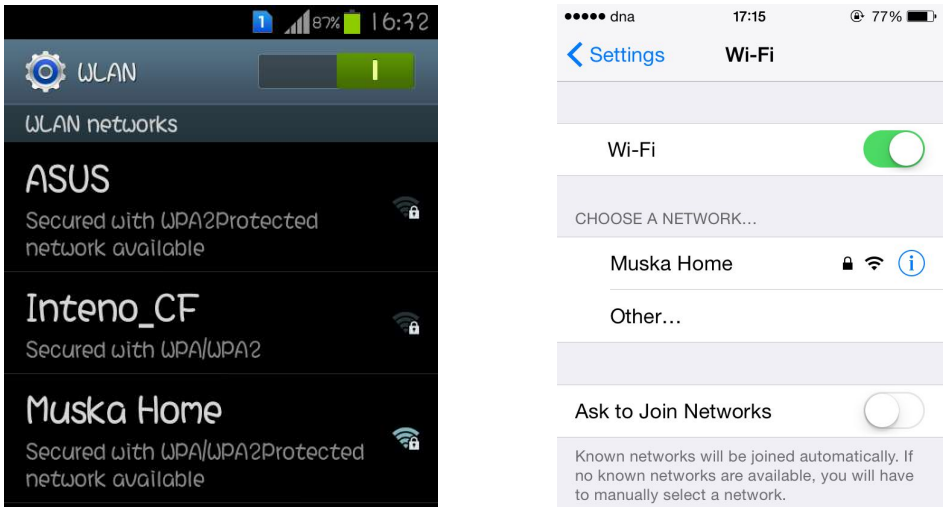

FIGURE 4. All available Wi-Fi networks available in two mobile devices

If the Wi-Fi network requires authentication, we should input the password for the connection (shown in Figure 5).

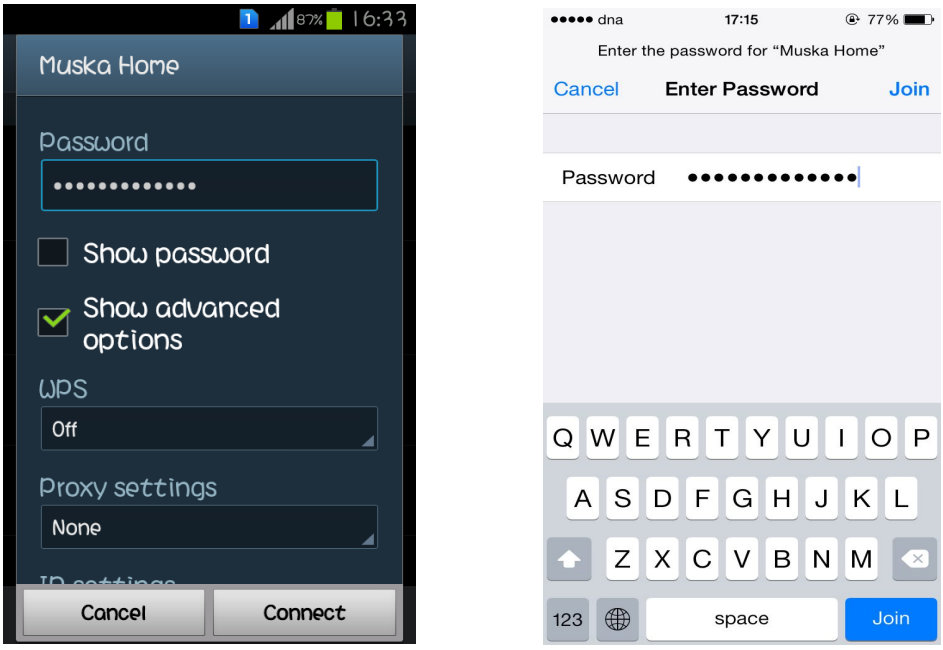

FIGURE 5. Input the password for encrypted Wi-Fi

Finally, the mobile devices can connect to this Wi-Fi network successfully. We can see that there is a logo appeared shows signal strength and connected to this network (shown in Figure 6).

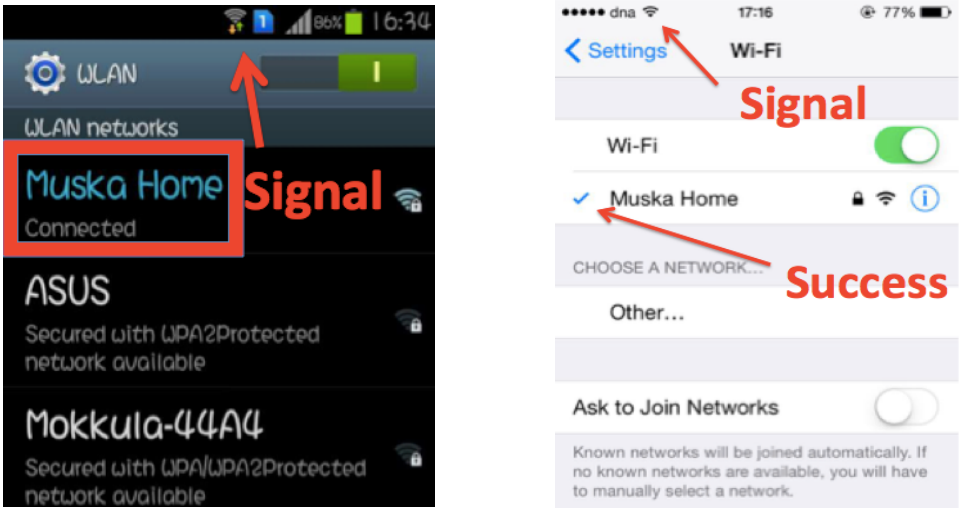

FIGURE 6. The mobile devices connected to a Wi-Fi network successfully

Over all, it is not difficult to find out that the method to connect to the Wi-Fi network in iOS mobile devices is similar to that of Androids.

3. SECURITY TECHNOLOGIES IN WLAN

There are multiple security objectives. Typically, the security technologies for mobile devices in a Wi-Fi network include confidentiality, integrity and authentication.

3.1. Confidentiality and Integrity

Confidentiality ensures an unauthorized party will not read to communications between the mobile device and the Wi-Fi network. Integrity detects any intentional or unintentional changes to data that occur in transit.

The threats for mobile devices to use Wi-Fi network mainly from untrusted third party behind by attack, copy, stolen or change information. Cybercriminals always try to find a tunnel to access mobile device. The wireless communication with an exposure transmission improved the level of vulnerabilities compared to wire one. Therefore, the data transmitted at an open Wi-Fi network is easily eavesdropped, lost or stolen by an unknown third party. Hackers could acquire our private information, E-bank details, online accounts, etc.

The purpose of confidentiality technology is to hide information when data is transferred over the wireless network, and to ensure that unauthorized parties cannot read transmitted and stored data. This security technology for Wi-Fi network includes three ways: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2).

3.1.1. WEP

WEP was certificated by the Wi-Fi Alliance as part of the original 802.11 standard in 1999 to protect data confidentiality in wireless network. WEP uses RC4 to encrypt the data passed over the network. RC4 requires a passphrase that is made of two parts. The first part is a pre-shared key (PSK) must be entered into the configuration settings (generally 5 or 10 characters in length) of each node before connecting to the wireless network. The second part is a three-character initialization vector value (IV) that in used to encrypt each packet with a different key. This value is sent pre-pended to the packet as plaintext that the receiver strips off and uses in the decryption process. However, IVs were not exclusive. Once they were created using the passphrase as one of the variables, the plaintext IVs statistically leaked the PSK, so that attackers can extract passively sniffing encrypted packets. (Fogie, 2003)

WEP is the weakest encryption method compared to the other two confidentiality technologies. However, WEP has been widely used for a long time, because it is available for all 802.11 standard wireless products. Fortunately, WPA and WPA2 are replacing WEP and have already made a program. Therefore, I highly recommend using WPA and WPA2 instead of WEP in Wi-Fi encryption.

3.1.2. WPA and WPA2

In response to the vulnerabilities found in WEP, WPA was defined. WPA is known as the draft IEEE 802.11i standard, typically to support multiple variations of the WPA technology. WPA is also regarded as an intermediate measure in the anticipation of the availability of the more secure and complex WPA2. WPA inherited the basic principle of WEP and improved WEP's shortcomings. WPA utilizes the Temporal Key Integrity Protocol (TKIP) to generate the encryption key, which is dynamic key that was not supported with WEP and RC4 for encryption. Therefore, even if the attacker collects a lot of packets, it is almost impossible to calculate the common key. WPA also creates an additional function to prevent data tampering and authentication. In a word, WPA is a much more powerful encryption method than WEP.

However, some vulnerability in the TKIP method used with WPA was found later. In order to response to these vulnerabilities, the full IEEE 802.11i standard was developed. Wi-Fi Alliance applied this standard and referred to it as WPA2 in 2004. WPA2 includes mandatory support for CCMP based on the AES (Advanced Encryption Standard) encryption mode with strong security. WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark. Finally, WPA2 includes authentication, encryption and data integrity, which is a complete security program. (Wilkins 2011)

Different WPA versions and protection mechanisms can be distinguished based on the version of WPA, the target end-user, and the encryption protocol used. WPA-Personal mode is also referred to as WPA-PSK (Pre-Shared Key) mode. It is designed for family and small office networks and does not require an authentication server. Each wireless network device is authenticated with the access point using the same 256-bit key generated from a password or passphrase. Organizations usually use as encryption protocol WPA-Enterprise that is designed for enterprise Wi-Fi networks. WPA-Enterprise requires a RADIUS (802.1X) authentication server, a more complicated setup to ensure an additional security.

3.2. Authentication

Except the confidentiality technology, authentication technology is another important security insurance which guarantees that the wireless network is only accessed by authorized mobile device users. There are three main methods of authentication on today's wireless LANs: Open System and Shared Key authentication, WPA and WPA2 with Pre-Shared Keys authentication, and finally WPA and WPA2 with Enterprise authentication.

Both Open System and Shared Key authentication methods are used together with WEP encryption. Open system authentication is the simplest method allows any user to authenticate them to the access point as long as the device knows the Service-Set Identifier (SSID) of this network. While SSID is typically send as a broadcast, it can be easily figured out with passive capturing techniques. Shared Key authentication is commonly used on family and small office wireless networks. It uses a shared key given to both sides of the connection. Once they match the wireless network, the device is allowed onto the network. Share Key authentication can be used only with WEP encryption, and therefore it is not considered a secure method of granting network access. (Wilkins 2011)

WPA (PSK) and WPA2 (PSK) Wi-Fi Protected Access methods use pre-shared keys for authentication. WPA and WPA2 PSK authentication are more secure than WEP Shared Key authentication. The network devices could configure a pre-shared key by WPA only, WPA2 only or WPA/WPA2. These methods allow users who know this key to have access onto the network.

WPA and WPA2 enterprise authentication methods use the IEEE 802.1 X standard, which is more secure than WPA and WPA2 with Pre-Shared Keys authentication. They use the EAP (Extensible Authentication Protocol) framework to enable user authentication to an external RADIUs authentication server, so that users authenticate themselves with their own credentials instead of a shared key. Similar to the Pre-Shared Keys authentication, the network devices can be configured to use WPA enterprise authentication, WPA2 enterprise authentication or WPA/WPA2 enterprise authentication. (Watchguard 2015)

3.2.1. IEEE 802.1 X

IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC), and also a subset of the IEEE 802.1 group of networking protocols. It

provides authentication for mobile devices attached to a wireless network. Simply speaking, 802.1X authentication included three parties: a supplicant (the mobile device), an authenticator (the enterprise Wi-Fi network), and an authentication server (the host running software supporting the RADIUS and EAP protocols). Before the supplicant access the enterprise network, the authenticator will work as a security guard for the verification of the supplicant's user account or digital certificate. If the credentials are valid, the supplicant is allowed to access the network (shown in Figure 7).

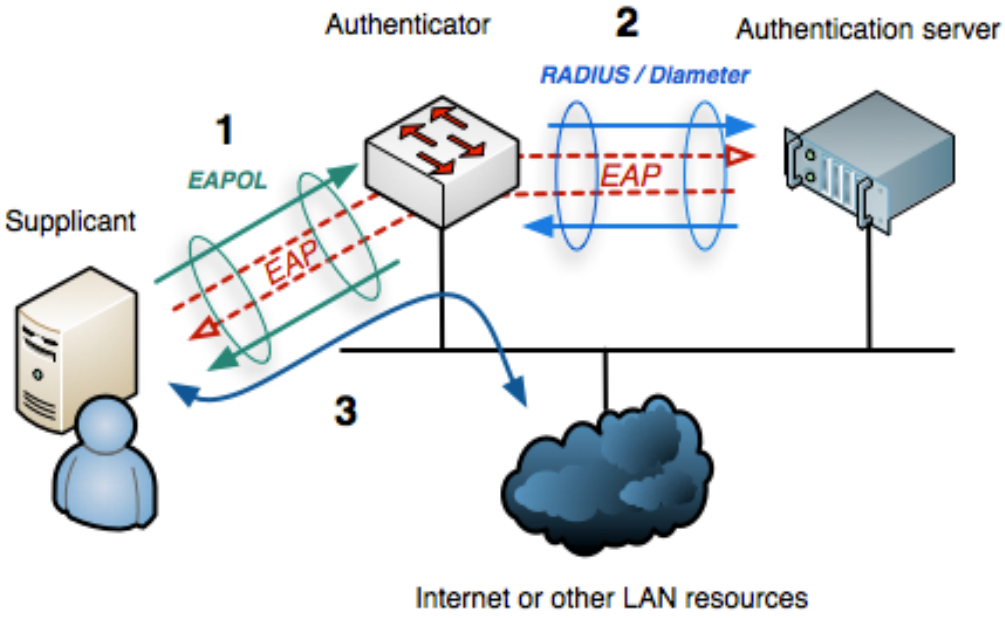

FIGURE 7. Authentication process

4. INDIVIDUAL USER IN WI-FI NETWORKS

In this chapter I mainly talk about the risks for mobile devices inside a Wi-Fi environment. Firstly, I introduce the scope of individual mobile device users in this thesis. Next, I talked about how different risk situations might affect individual users. In addition to that, I give suggestions for individual mobile device users and a summary of the security solutions.

4.1. Overview of an Individual Mobile Device User

In general, users use mobile devices in environments like public hotspot Wi-Fi, commercial Wi-Fi or household Wi-Fi. This kind of users is being called individual mobile device users. Because the administrator of the household Wi-Fi is usually the user of the mobile device, and cybercriminals must be physically close to the household Wi-Fi, the risk of household Wi-Fi is small. Therefore, the home based Wi-Fi networks are not discussed in this thesis, and the Wi-Fi environments I discuss in this chapter are limited only to tree or commercial public Wi-Fi networks.

In order to meet the demands of individual mobile device users, some airports, libraries, universities and other public places also build their own hotspot for public. An increasing number of hotels and restaurants provide free Wi-Fi for customers, so that customers could get access to an available Wi-Fi network with their mobile devices. The facts demonstrate that a café with a free available Wi-Fi is more attractive than those without Wi-Fi for customers.

With the growing number of mobile device users connecting to Wi-Fi, there is a dramatic growth of risks. Cybercriminals intrude mobile devices, and steal users' private information, e-bank account etc. The British Daily Mail reported on January 21, how a 7-year-old girl named Besty Davies successfully cracked the password of a Wi-Fi hotspot within 11 minutes after watching a tutorial video from YouTube. A VPN vendor who organized this experiment that child attacked a public Wi-Fi network wanted to emphasize the network security issues. (Dailymail 2015)

In the summer 2013 Kaspersky Lab joined forces with international research agency B2B International to conduct a new survey that included 8,605 respondents from 19 countries. According to this survey, 70% mobile devices users use free public access points. However, 34% respondents stated that they do not take any additional security measures when they

connect to public hotspots. Another 14% stated they are not concerned about using public Wi-Fi to process personal financial data, such as online stores, online banking services, and e-payment systems. Only 13% of the surveyed mobile device users said that they asked about the encryption standards used before connecting to hot spots with their personal devices. (Kaspersky 2013)

4.2. Risk Statement

The cyber threats for mobile devices under the public Wi-Fi environment include: financial loss, data leakage, password or personal information theft, etc. Hacker tries to get access to mobile devices via wireless networks by using different measures to eavesdrop or copy the information to reach their goal. General criminal ways of Wi-Fi hackers include: evil twin, man-in-the-middle, malware, and data theft. The following section introduce these hacker methods in detail.

4.2.1. Evil Twin

An evil twin is a rogue Wi-Fi access point, which looks like a legitimate Wi-Fi hotspot. But actually, it is a tainted hotspot set up by a hacker to fool mobile device users' connection. As Figure 8 shows, only the path 1 connects to the secure Wi-Fi network. Hackers try to use a rogue Wi-Fi by a similar name like 'McDonalds guest', while the official one is named 'McDonalds' required for online registration. Once you connected to the rogue Wi-Fi network using path 2 in Figure 8, it means that your mobile device is in danger.

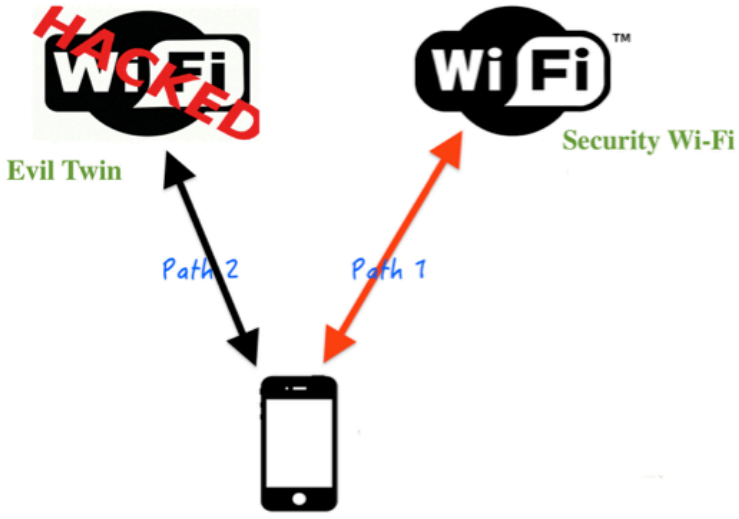

FIGURE 8. Evil twin

Evil twin could be regarded as the wireless version of the phishing scam, aim to capture users' passwords and other sensitive information. Most mobile devices trust the Wi-Fi network they connected, so that it gives permission for the Wi-Fi network servers to listen to all this mobile device's Internet traffic. Once the mobile device users log into a non-HTTPS financial account, hacker has access to the user's transaction. (Private WiFi 2014)

However, the only way to prevent connection from the evil twin Wi-Fi access point is by artificial distinguishing and most people only concentrate on the available Internet without being aware of rogue Wi-Fi networks. Therefore, evil twin gives hackers a flexible space and improved the risks for mobile device users to use an unknown public Wi-Fi network.

4.2.2. Man-In-The-Middle

Man-in-the-Middle (MITM) attack is executed by a hacker's third party device between a mobile device and a Wi-Fi network server (shown in Figure 9). Once the third party device intercepts the original path 1 of data communication between the mobile device and the legitimate network access point, hackers could obtain mobile devices' authentication credentials through this third party device. Even worse, hackers could masquerade as an authorized and legitimate party to eavesdrop or even modify mobile device users' information.

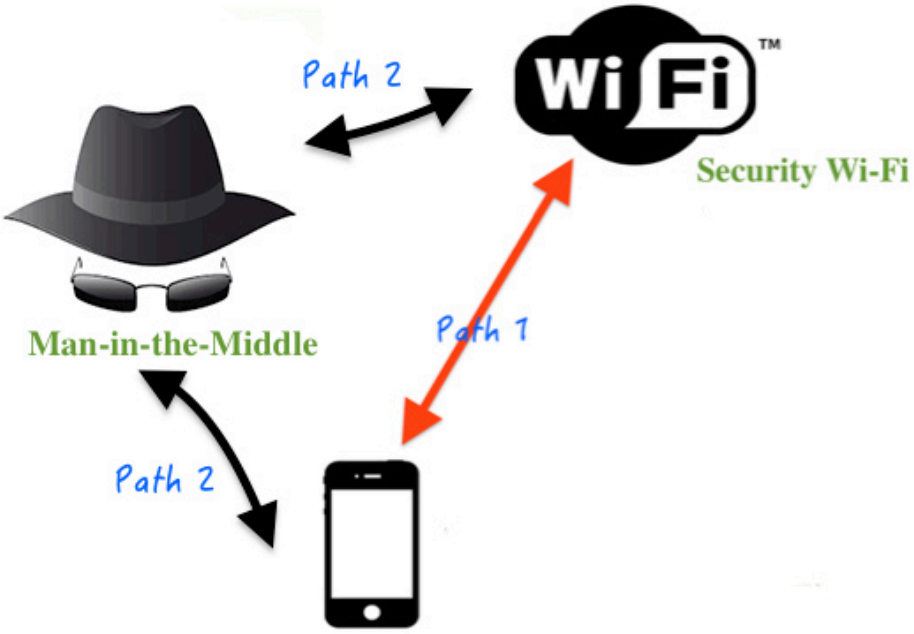

FIGURE 9. Man-in-the-Middle

Sniffer software is one of the third party devices for man-in-the-middle attacks to intercept message. Sniffer software can capture e-mails, web messages, or files transferred when they are passing through the wireless network.

4.2.3. Malware

Malware (malicious code) usually caused by security breaches or damage to a system. There have been instances of travellers being caught off guard when connecting to public Wi-Fi networks when their device prompts them to update a software package. If accepted by the user, malware was installed on the machine.

Malicious programs is a major problem that affected individual mobile device users, while 13% of tablet owners and 10% of smartphone owners reported that their device had not worked properly at some point due to malware. (Kaspersky, 2015)

4.2.4. Data Theft

The data sent from mobile devices over the Wi-Fi network could easily being captured by eavesdroppers. Mobile devices are now frequently used to store critical data, which include online finances, commercial confidentiality, personal online accounts, or even private information. Mobile device users also store personal photographs, videos, and audio files. Because people often use mobile devices to access all types of online services, it brings a major data security threat for mobile device users when an Internet connection is established via Wi-Fi.

About 22% of smartphone owners (not including iPhone owners) store information needed to access their personal email accounts, and another 32% even store their work email account information on their phones. Tablet owners (not including iPads) do the same: 29% store their work documents on these devices, while 28% store work email information, and another 23% store the information needed to access their personal email accounts. (Kaspersky 2013)

4.3. Security Measures for Mobile Device

Many individual mobile device users tend to be unaware of security measures. They use mobile devices to collect, access, and process large amounts of valuable and sensitive information on a public Wi-Fi network. Even though some of the mobile device users realize the risks of using a public Wi-Fi network, it is difficult for them to figure out what kind of

dangers they are facing before they connect to a free available Wi-Fi network. Fortunately, there are some security measures, which could help individual users to reduce the risks when using public Wi-Fi networks.

4.3.1. Verify The Network Name

Reaching to a secure object for mobile devices, the first step for users is connecting to a reliable network. If the users are not sure about the official network in a cafe or a restaurant, they should ask the employees and carefully check that it matches the one in the device's Wi-Fi menu to avoid the mobile device fall into an illegal hotspot. As mentioned earlier, the evil twin Wi-Fi network should be figured out manually. Hence, connecting to the legitimate access point by choosing the right full name in the device's Wi-Fi menu could reduce the risk of evil twin connections.

4.3.2. Disable the Connection Automatically

Except to trap users by using a similar name of an official Wi-Fi network, evil twin Wi-Fi hotspots attract mobile device connections with easy access. Most mobile devices have a possibility to automatical connection creation. This option is disabled by default, while some users have opened the automatical connection for convenience and forget to disabled when their device is in dormant state.

Once a mobile device user set automatically connects to any available Wi-Fi hotspot, this mobile device might be connected to the evil twin in an unknown situation without permission. Therefore, mobile device users should disable the Wi-Fi connection (as shown in Figure 4 of Section 2.3.2) after they do not need it. It could be the best way to prevent hackers.

4.3.3. Check 'HTTPS' in URL Bar

The best way to prevent important information from Man-in-the-Middle attacks is using end-to-end encryption. HTTPS which refers to Hyper Text Transfer Protocol over Secure Socket Layer is a communication protocol which provides authentication of the visited website and deploys secure communication over a network. This protocol is especially widely used on the Internet.

Regular websites transfer content in plain text, which makes it easier for a hacker to reach his target. Today, many websites use HTTPS to encrypt the important data or financial information. (Berg, 2013) Once the user is connected to a HTTPS website, the browser will display a padlock icon in the address bar which stand a SSL connection is active. SSL protocol has long been standard for financial institutions, and it enabled when mobile device users reaches a login page, view the account information, or enter payment bills. (Diallo, 2014)

Commonly, the browser would give warning of untrusted site with red color in address bar. In case of Man-in-the-Middle already get into the Wi-Fi network and aimed to attack the mobile devices, users should never ignore the HTTPS in the URL bar when they deal with sensitive information.

4.3.4. Use a VPN Service

As another end-to-end encryption method, Virtual Private Network (VPN) services convert the plaint text into unreadable codes.

VPN services create a physical barrier by routing all the communications between the mobile device and the Internet. Otherwise, the communications is transmitting from the mobile device directly to the Internet as a plain text like Figure 10 demonstrates, which could be easily intercepted by a third party. This gives a huge possibility for Man-in-the-Middle hackers to access the mobile device user's traffic, reading the information that tied via the IP address in the mobile device. (Diallo, 2014) With the physical barrier, all the traffic could realize automatically end-to-end encryption between the mobile device and the VPN service. (Shown on Figure 10)

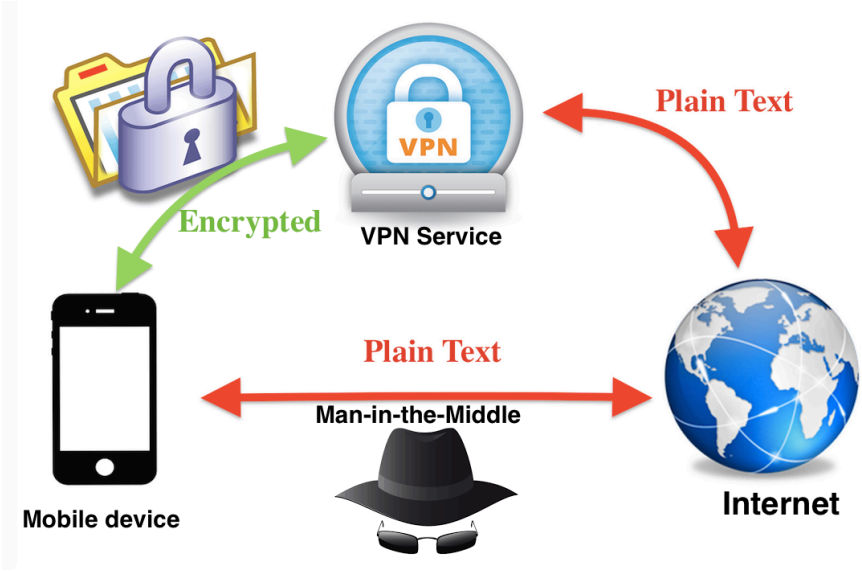

FIGURE 10. VPN Service

There are a lot of VPN services now available in apps for both Android and iOS mobile devices. No matter the VPN service you choose is free one or charged one, I hope you could install the VPN app from official app store such as Google Play store or Apple App store.

4.3.5. Anti-Virus app

In order to prevent against the malicious code, anti-virus app has been used to protect mobile devices.

Anti-Virus app is a real-time malicious programs monitor and scanner. Most of Anti-Virus apps like AVG and Kaspersky have self-protection mode, which is working as a firewall for mobile devices to detect malware automatically. Once the Anti-Virus app detects a new malicious code, it will by default remove those viruses, worms, and Trojan from the mobile device. In addition to that, Anti-Virus app also have repair technology, which could repair the corrupted files or programs and reduce network vulnerabilities.

Always running the Anti-Virus software on the mobile devices could help to provide the first alert once the system has been compromised while connected to an unsecured Wi-Fi network. The alert include any suspicious or recognized virus, which loaded onto the mobile device already.

4.3.6. Two-factor authentication

As a security technology to protect mobile devices, mobile two-factor authentication was developed to avoid data theft. If users want to authenticate themselves, they can use their personal accounts plus a one-time-valid, dynamic passcode consisting of digits. The code can be sent to their mobile device by SMS or via a special app.

The mobile two-factor authentication stop hacker who have stolen your password to login to your accounts, because of another necessary code can only be ready in your mobile device. Some financial companies already provide the two-factor authentication for their customer's online accounts. Some online drives that are used to store files in an online account need special settings of the two-factor authentication for the high secure level files. I strongly suggest using two-factor authentication as much as possible to protect your online information.

5. ENTERPRISE WI-FI NETWORK SECURITY

This chapter mainly focuses on the enterprise Wi-Fi network. First of all, there is an introduction of enterprise Wi-Fi network environment. Next, the possible risks for mobile devices for the enterprise Wi-Fi will be list. In addition to that, some relative security measures will be indicated in the end of this chapter.

5.1. Enterprise Wi-Fi Network Overview

Enterprise Wi-Fi network is a wireless local area network using multiple access points without wired links. Therefore, all the mobile devices could connect this network through any access points. Enterprise Wi-Fi network have completed the enterprise wired network environment and become popular among small and medium business enterprises including business companies, administrative apartments, schools, etc. Furthermore, a growing number of business hotspots are updating from personal Wi-Fi networks into enterprise Wi-Fi networks, such as hotels, airport and so on.

People are using wireless network instead of wired network for better convenience, which is same purpose of personal Wi-Fi network. Enterprise requires higher security level to prevent the malicious attacks, especially for some administrative apartments. Enterprise Wi-Fi network usually have an internal access controls for mobile device users, so that only authorized mobile devices have permission to use network resources.

In the past few years, enterprise Wi-Fi usage increased with a rapid speed because the development of BYOD. In order to perceive productivity gains and cost savings, companies encourage their employees to bring their own devices. Chris Ross, Managing Executive of Products and Services at Vodacom Business said: “With around 95% of employees stating they use at least one personal device for work, BYOD is a reality that company network security managers simply cannot ignore.” (Vodacom, 2015) Therefore, mobile devices are becoming the main channel for cybercriminals, as well as the Wi-Fi network is undoubtedly the largest security risk.

The risks for enterprise Wi-Fi network mainly from the hacker attack the network through mobile devices, which get the permission into this network. Similarly, hacker utilized the wireless waves as their tunnel to reach their object, so that the protection job becomes difficult. The following content will give a discussion of the dangerous effect for enterprise

Wi-Fi networks from mobile devices and relative protection solutions.

5.2. Risk Statement

Mobile devices are used in a variety of locations out side the organization's control, such as coffee store, hotels, and user's house. Even though some mobile devices only used within an organization's Wi-Fi network are transported from one place to another within the facilities. Hence, the risk of enterprise Wi-Fi network would increase by mobile devices acquired malicious from the third parties.

There is no answer for what are the greatest threats for enterprise Wi-Fi so far, but one thing we can make sure is that mobile devices became the biggest intermediate tools for hackers to infiltrating the enterprise Wi-Fi network. Similar to the purpose of last chapter mentioned in the risk statement of mobile devices, the risk from mobile devices to the enterprise Wi-Fi network include access attacks and spying attacks. In addition to that, hackers also intent on availability attack.

5.2.1. Spying Attacks

Spying attacks for the enterprise Wi-Fi networks could known as reconnaissance, it is the unauthorized discovery and mapping of systems, services, or vulnerabilities. Hacker relies on moving mobile device search information in the neighboring areas of an enterprise Wi-Fi network in which behavior is similar to a thief scouting a neighborhood for unsecure houses. They utilize the wireless protocol analyzer to scan the enterprise Wi-Fi network by transmit no information while they are detecting, so that they could eavesdrop on the enterprise Wi-Fi networks. (Matti's presentation, 2015)

Wireless reconnaissance often called Wardriving is illegal in some countries, while some countries do not make rules to limit because it also could be used in positive way. Wardrivers use Wi-Fi equipment together with GPS device to record the location of each Wi-Fi networks. After results processed into data and uploaded to the map website, there will form maps of network IDs, which can be used as a location systems of alternative to GPS — by triangulating the current position from the signal strengths of known network IDs. (Wikipedia, 2015)

5.2.2. Access Attacks

Another target of hacker to attack the enterprise is realized activity monitoring, data retrieval, illegitimate network connection or systems modifications, all this attacks could constitute a great threat for organizations. In order to do this, hacker must gain the access ability of an enterprise Wi-Fi network system by their unauthorized identities first.

One way of access attacks is using the gathered information through reconnaissance. With that information, hacker can exploits the vulnerabilities of an enterprise Wi-Fi network system via a mobile device, running together with a hack script or tool. Thereby hacker could obtain the ability to access enterprise Wi-Fi network as an unauthorized intruder without an account or password.

Another way to access an enterprise Wi-Fi network without authorized identity is by rogue access points, this method is similar to evil twin attacks for mobile devices in chapter 4.2.1. Hackers using an unauthorized access point with stronger signal, so that mobile device will associate to the rogue access point. Thereby, the rogue access point could access to the organization's network traffic of all associated mobile devices. (Shown in Figure 11) In addition to that, rogue access point can also use ARP (Address Resolution Protocol) and IP spoofing to trick mobile device users sending sensitive information and passwords.

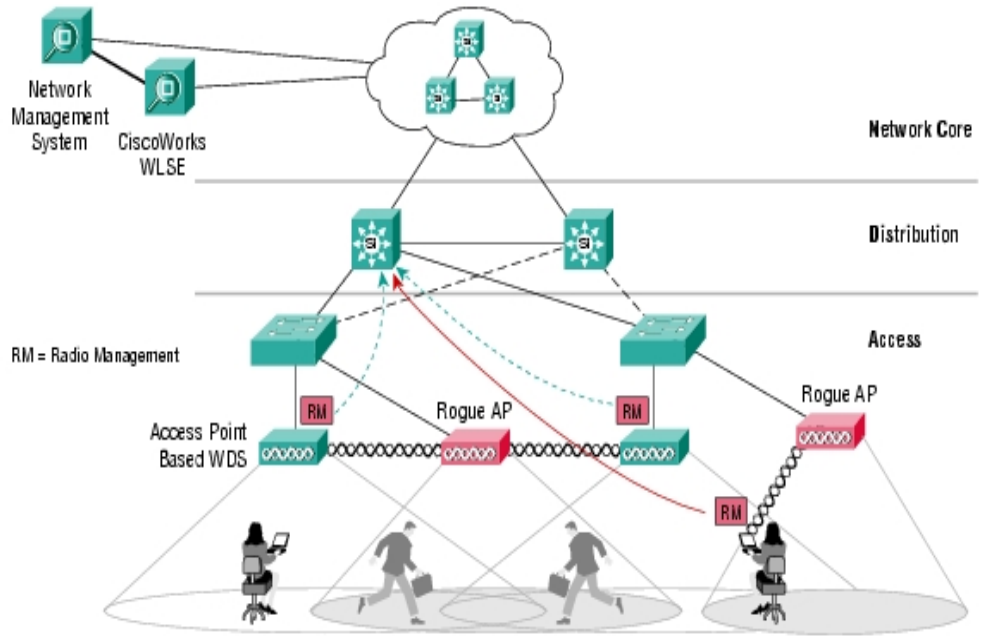

FIGURE 11. Rogue access point attacks (Matti, 2015)

Additionally, against WEP could be a way for hacker to access the access point for those organizations used WEP for encryption. WEP attacks the enterprise Wi-Fi network access points include Bit Flipping, Replay Attacks, and Weak IV collection. Hacker depended on utility to capture WEP data, and determine the key of WEP. As earlier mentioned in chapter 3.1.1, WEP should not be used in any secure case. (Matti's presentation)

5.2.3. Availability Attacks

Availability in wireless network security means network devices and individual mobile devices could access a network, in which the resources is available whenever users need. Availability attacks is an attempt to make an enterprise Wi-Fi network resource unavailable to its intended users. A denial of network availability for the Wi-Fi network involves some forms of denial-of-service (DoS) attack, such as jamming attack or flooding attack. Those threats are difficult to counter in any radio-based communications.

Jamming attack occurs when hacker deliberately emanates an RF signal from a mobile device to overwhelm legitimate organization's devices and signals, thereby signals from the organization Wi-Fi network sever are unable to be properly transmitted. Finally, jamming attack could result in a breakdown or complete loss of enterprise Wi-Fi network.

Flooding attack can also cause significant disruption to enterprise Wi-Fi network by attacks on access points and other enterprise machines. Hacker using specific software to transmit a large number of packets to access points via mobile devices, causing the access points to be overwhelmed by packets and cease normal operation. Flooding attack can cause the enterprise Wi-Fi network to degrade to an unacceptable performance level or even fail completely.

Additionally, Non-malicious mobile device users can also cause a DoS attack by unintentionally monopolizing the capacity of a WLAN by downloading large files, effectively denying other mobile device users access to the network. (NIST, 2007)

5.3. Security Measurements

For the sake of security, a multiply approach methods need be done for users' mobile device to protect the enterprise Wi-Fi network. Organizations should have a security policy for all mobile device users to prevent risks from mobile devices for the enterprise Wi-Fi network.

5.3.1. Controlling Mobile Devices Access

In order to prevent any types of mobile devices could access the network resources as easily as trusted mobile devices, organization could catalog diverse access levels to limit the available of resources for different mobile devices. For instance, organization-issued devices have ability to access most of resources, while personal-owned devices could only access a limited resources of all, other types mobile devices like visitors or gusts cannot access a few web-based resources such as email.

Controlling access level of information reduce the risk by limit the least-controlled mobile devices to access whole the enterprise Wi-Fi network, so that untrusted mobile devices can not get permission to access organization's sensitive information. There is not an exactly range of most-controlled mobile devices or least-controlled mobile devices, so that risk-based decisions about what levels of access should be permitted from which types of mobile devices is various from one organization to another. (NIST, 2013)

In addition to that, some organizations even could design a specified mobile devices management client app according to their security requirements, which could automatically verify the requirements from mobile devices and conduct security health checks. Therefore, only verified requirements through specified mobile device app can executed in that mobile device. The specified mobile device app not only can limit untrusted mobile devices without install management client app, but also build a guard for checking mobile devices' network requirements.

5.3.2. Association Process

After designed an access level for different types of mobile devices to ensure security, organization also should focusing on mobile devices association process as showed on Figure 12 especially authentication steps.

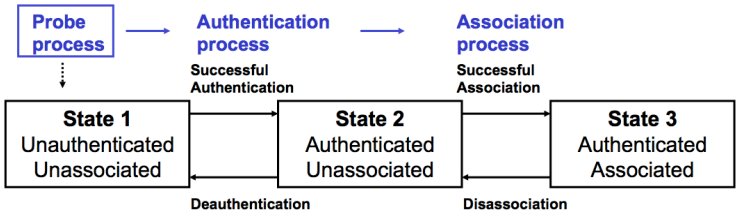

FIGURE 12. Mobile devices association process

As mentioned in chapter 3.2 authentication technology guarantees enterpriser wireless network only accessed by authorized mobile device users. As one of three authentication technologies introduced earlier, Open System and Shared Key authentication is typically for public Wi-Fi networks without verification user. When using WPA and WPA2 with Pre-Shared Keys authentication, access points will sends a challenge packet to the mobile device and allowed user who known this key access onto the wireless network. Pre-Shared Keys authentication ensures the security for home or office sized wireless network, while enterprise Wi-Fi network requires higher secure which only WPA and WPA2 with Enterprise authentication can reached currently.

Once the untrusted mobile device failed in authentication process in Figure 12 state 2, this mobile device association process would be unsuccessful, which means the untrusted mobile device cannot attack enterprise Wi-Fi network's passing by access onto access points.

5.3.3. Operation and Maintenance

Periodic maintenance is the basically needed for organization to check potential threats. It is helpful for organizations to do perform assessments to ensure mobile devices policies, processes and procedures are followed the organizations. This included reviewing logs, performance vulnerability scans, penetration testing, etc. Therefore, all the mobile devices and wireless network machines should updates and patches in regular time.

5.3.4. Additional User Requirement

Except operation for devices, building the security awareness for each mobile device user by training in side organization is key for execute all security measures. The training could be simple which object is cooperating organizations' security policies, so that mobile device users could follow the security rules of this organization.

6. IMPLEMENT CLIENTLESS VPN FOR A MOBILE DEVICE

After analyzing the mobile device security in theory both from the mobile device and Wi-Fi network perspectives in previous chapters, I implement one of secure communication solutions for mobile device users in this chapter.

This solution provides end-to-end security with SSL VPN. Because there is large number of different type of mobile devices, my implement is based on clientless mode. This method does not require any client application to be installed to the mobile device, but we can just use the normal web browser. In order to verify that mobile device uses VPN to convert the plaint text into unreadable codes, I implement a small-scale network. This chapter mainly records the result of my experiment.

Figure 13 shows the basic ideas of the my practice part, which include two access points, two computers, a hub, a switch and Cisco ASA5505 firewall. There are two networks, the left part is the outside network, the right part is the inside network. In the end, the mobile device would connect a secure way through the outside Wi-Fi network to the ASA firewall with VPN. From the ASA firewall the user is able to access the web management interface configure on the access point of the inside network.

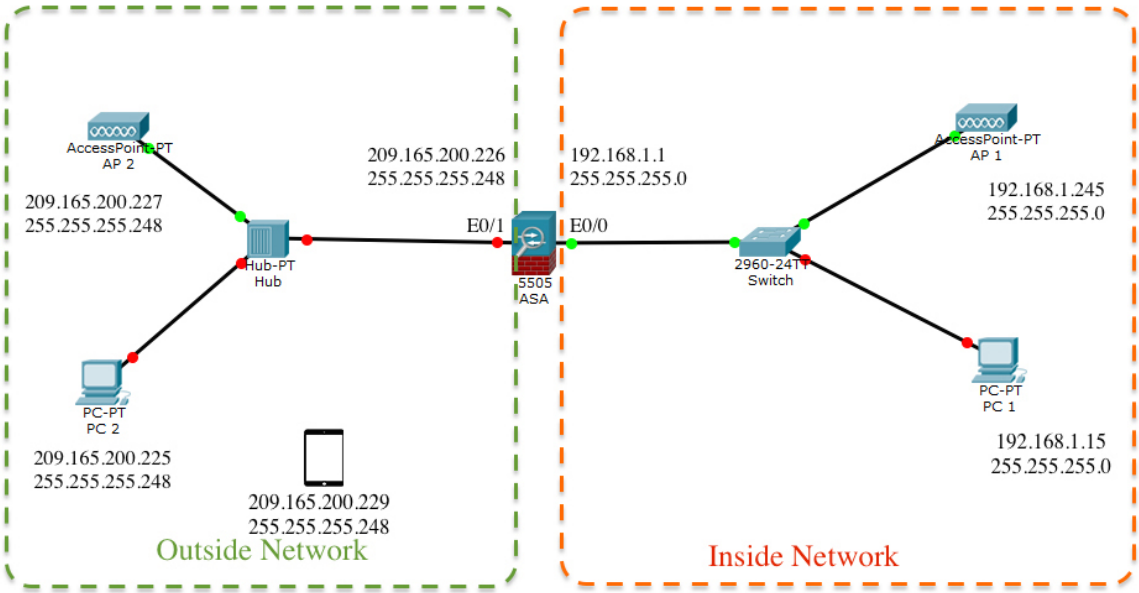

FIGURE 13. Practice networks

Firstly, I cabled the network and configure the IP addresses for all the devices. Then use Pre-VPN configuration Script commands to start configuring SSL VPNS for ASA. Therefore, when I open the browser in PC 1 and enter https://192.168.1.1, PC 1 could access to the ASA service through PC1's browser successful (shown in Figure 14).

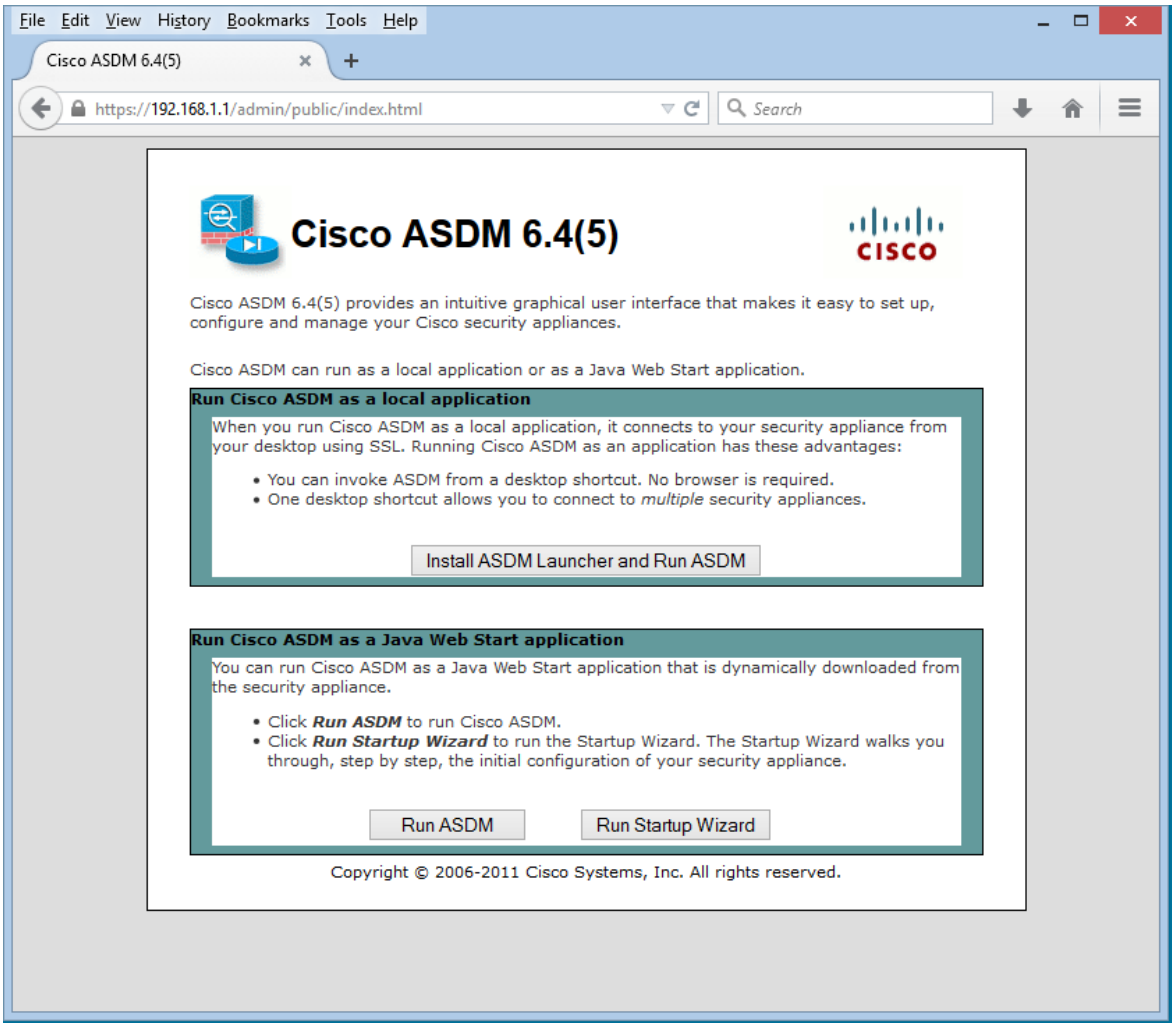

FIGURE 14. PC 1 access to the ASA through browser

Next, I run ASDM and start the SSL VPN Wizard configuration by choosing 'Clientless SSL VPN Remote Access'. Here I set the names and passwords, and add PC 2's IP address (209.165.200.225) in Bookmark (shown in Figure 15).

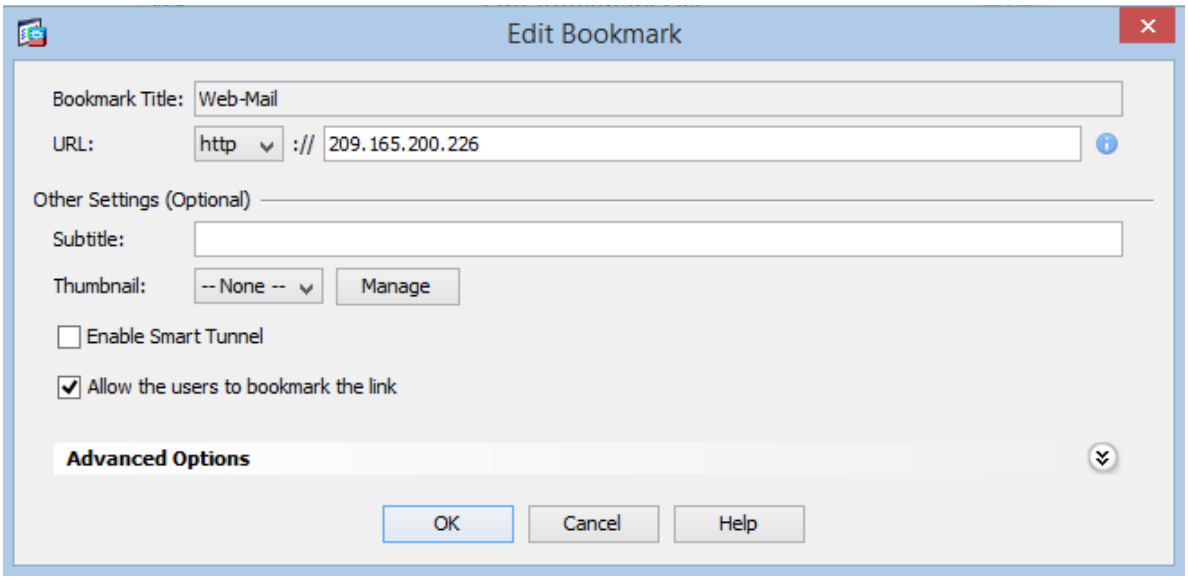

FIGURE 15. add PC 2's IP address in Bookmark

The SSL VPN Wizard configuration is shows as Figure 16 with the username is **UserHong**.

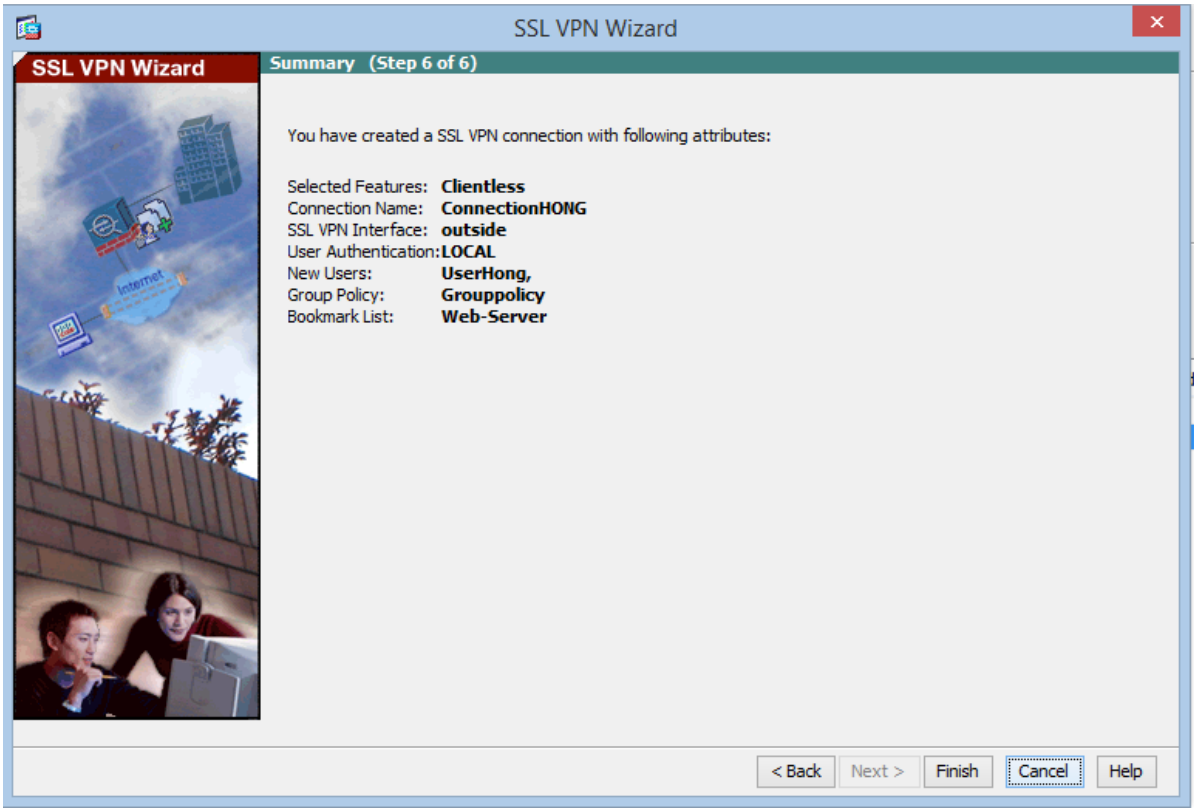

FIGURE 16. SSL VPN Wizard configuration

6.1. Testing The Clientless VPN From PC 2

In this section, I tested the clientless VPN from wired PC of the outside network (PC 2) and reported the results. Now, I enter the IP address (https://209.165.200.226) of the port connecting from ASA to the outside network in PC 2's browser. The login box will display (shown in Figure 17).

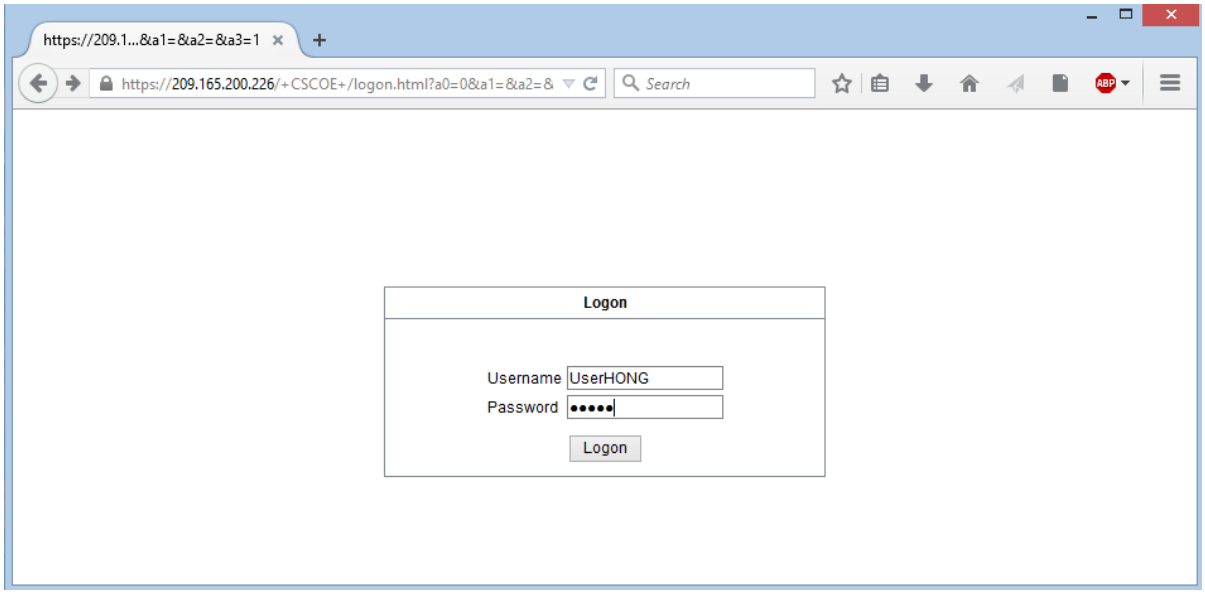

FIGURE 17. Login box when entering https://209.165.200.226 in PC2's browser

Login as user **UserHong** with its password, the Figure 18 will displayed in browser.

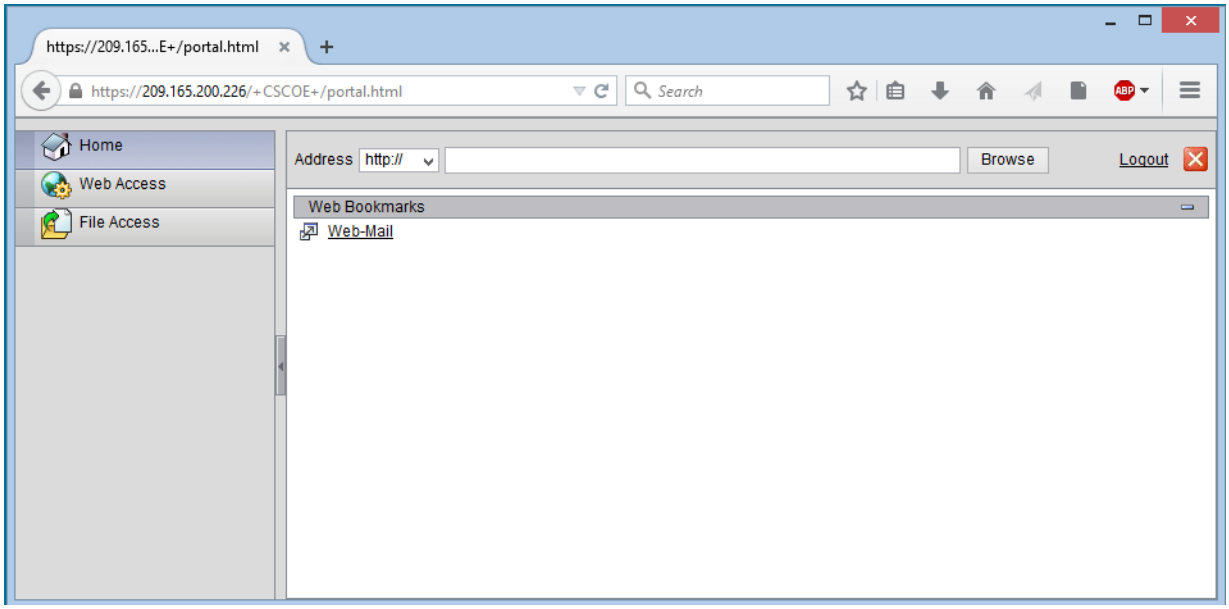

FIGURE 18. Login SSL VPN Wizard's account in PC 2

The browser of PC 2 could from outside network get into inside network. For example, when entering AP 1's IP address (192.168.1.1) in the address box, the browser could visit AP 1 (shown in Figure 19).

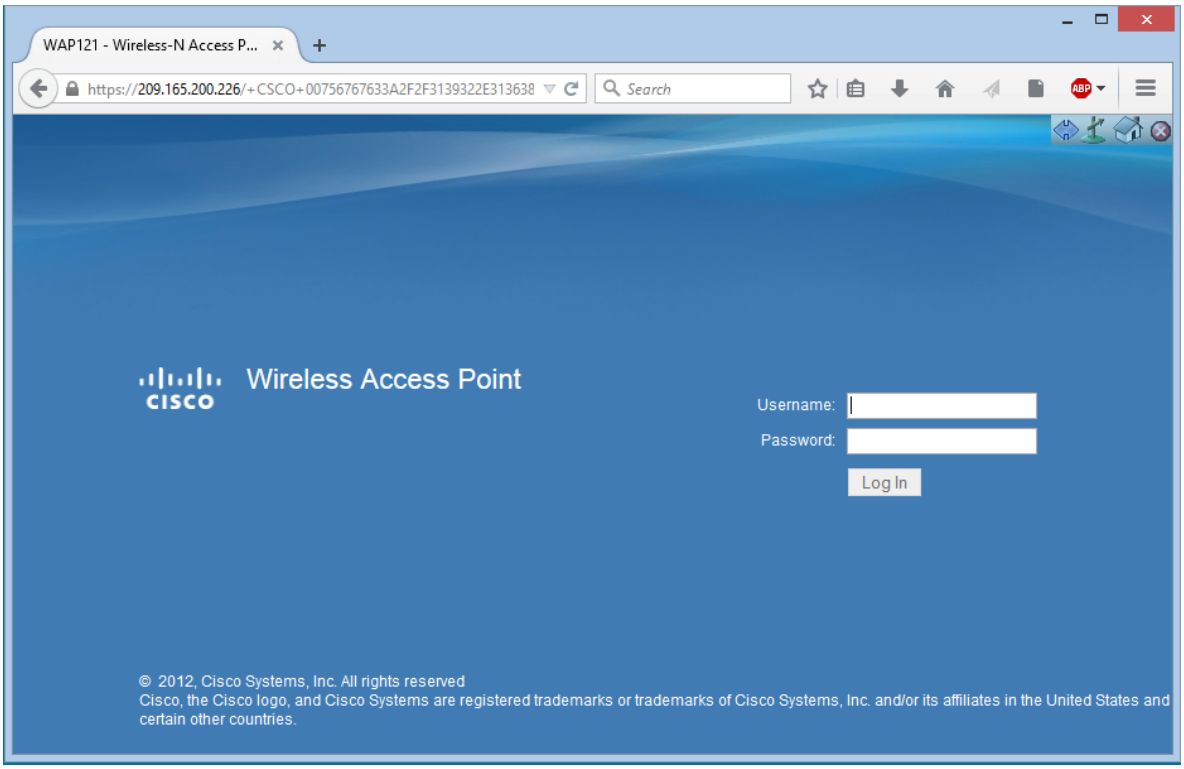

FIGURE 19. PC 2 could visit AP1 of inside network through VPN

6.2. Clientless VPN connection from a mobile device

In the previous section I tested the operation of the SSL VPN from the wired PC. Now it is time to test the connection from the mobile device. The mobile device I use in this experiment is iPad mini 2 with iOS operating system.

First, I configure the mobile device with the IP address 209.165.200.229 and default gateway 209.165.200.226 (shown in Figure 20).

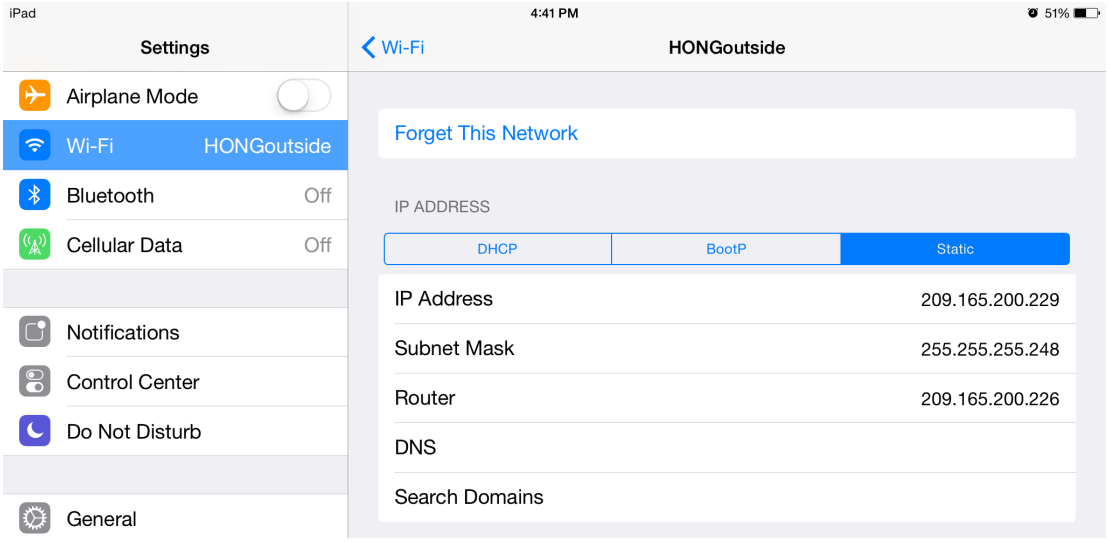

FIGURE 20. Configure IP address for mobile device

When I report the steps of the earlier section and enter the IP address of the ASA firewall, the result is similar to Figure 17, 18 and 19. During this time, the PC2 can capture the following information (shown in Figure 21).

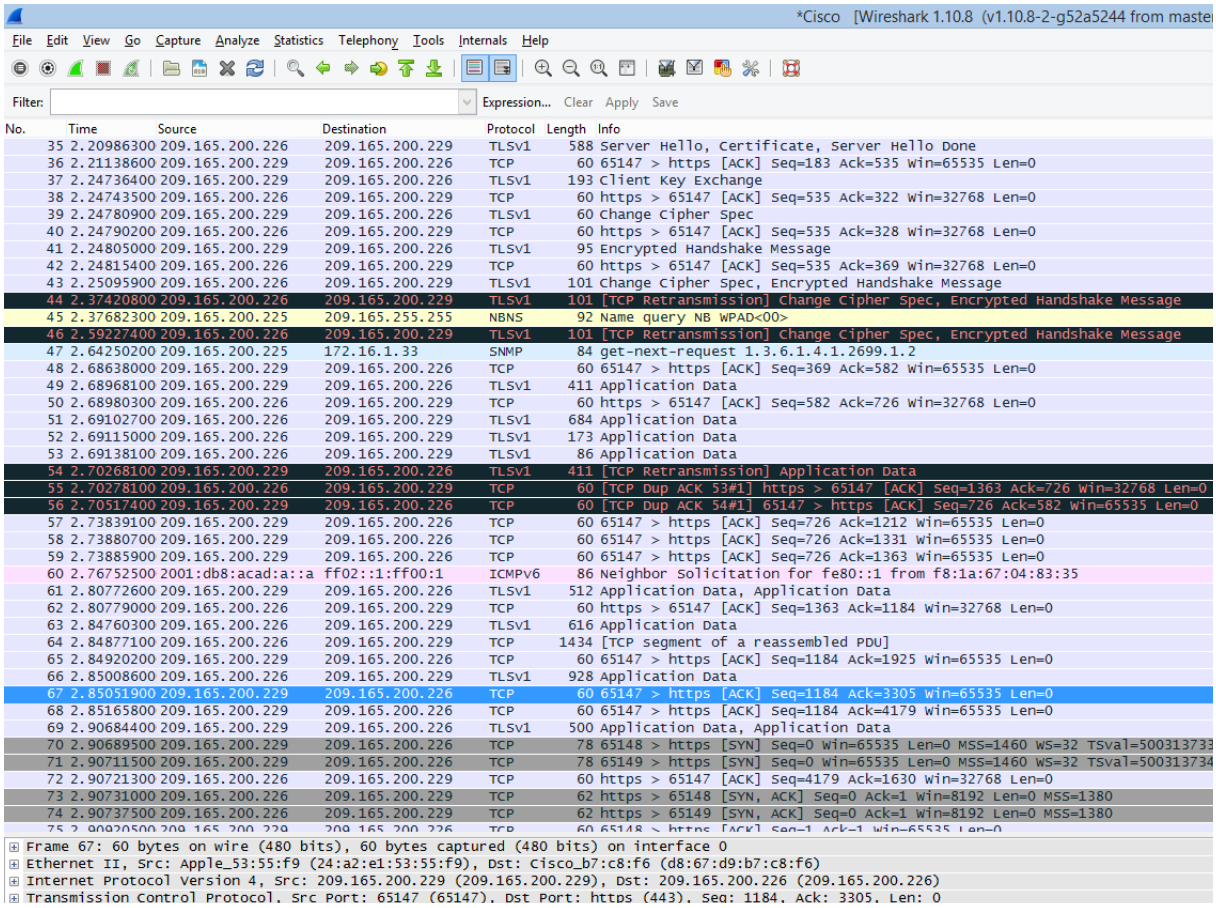

FIGURE 21. Captured information in PC 2

From Figure 21, we can see the SSL VPN client of the mobile device encrypted the traffic, so that the information captured by PC 2 is encrypted. Therefore, as earlier mentioned in section 4.3.4, when using a VPN service in the Wi-Fi network the traffic will be encrypted between a mobile device and a VPN sever.

7. CONCLUSIONS

Since smart mobile devices came into our daily life, wireless networks are replacing wired networks for users to connect to Internet. Therefore, the threats for important information, financial accounts and sensitive files transferred from mobile devices via Wi-Fi environment are growing. The aim of this study was figure out the security solutions for mobile devices and Wi-Fi networks which included theory part and practical part.

The theory part of this study included general introduction about mobile devices and Wi-Fi networks. Because of the attack target for hackers utilized the wireless network could be both mobile device user and Wi-Fi network of organization. The threats situation discussed divided into threats for mobile devices in the Wi-Fi network and organization against hackers use mobile devices through Wi-Fi network to attack their system. In the end, I gave security solution and my suggestions to prevent hackers' attack.

In spite of the overview in the theory part, the practical part mainly focus on verify if Virtual Private Network could guarantee the data confidentiality of mobile devices. In order to avoid varies VPN application services by different types mobile devices, I choose clientless mode of VPN. Finally, the traffic of mobile devices was encrypted into unreadable code between mobile devices and VPN server. The result of the practical part verify one of security solutions for mobile device users which could use the encryption between VPN sever and mobile devices to prevent data theft from hackers in the Wi-Fi environment.

Even through the security solutions I mentioned in my study is enough as a security guide for mobile device users and enterprise Wi-Fi networks at this era. There still would appear new threats cannot be forecast from hackers with the development of telecommunications. Therefore, this thesis might limit to use for the mobile device users at today. In addition to that, the limitations of my study also covered in practical part. There are a lot of security solutions for mobile device users, while I only verify one of them, if the time is enough, to verify all the security solutions and show their principle would be more perfect.

Overall, I satisfied with this study, not only because it showed my study result in MAMK, but also because it is very useful for the modern time.

BIBLIOGRAPHY

Berg, 2013, 9 Tips to Stay Safe on Public Wi-Fi, [referred 01.02.2013]. Available in www format:
http://blog.laptopmag.com/9-tips-to-stay-safe-on-public-wi-fi

Dailymail, 2015, Hacking Wi-Fi is child's play! [referred 24.02.2015]. Available in www format:
http://www.dailymail.co.uk/sciencetech/article-2919762/Hacking-Wi-Fi-s-child-s-play-Seven-year-old-shows-easy-break-public-network-11-minutes.html

Diallo, 2014, How to avoid data theft when using public Wi-Fi [referred 07.03.2015]. Available in www format:
http://www.forbes.com/sites/amadoudiallo/2014/03/04/hackers-love-public-wi-fi-but-you-can-make-it-safe/
Want Privacy On The Internet? Then You Need A VPN [referred 07.03.2015]. Available in www format:
http://www.forbes.com/sites/amadoudiallo/2014/03/07/want-privacy-on-the-internet-then-you-need-a-vpn/

Fogie, 2003, WPA Part 2: Weak IV's [referred 23.05.2003]. Available in www format:
http://www.informit.com/guides/content.aspx?g=security&seqNum=85

Gizmodo, 2007, Live: Google's gPhone Open Handset Alliance Conference Call [referred 07.05.2011]. Available in www format:
http://gizmodo.com/318561/live-googles-gphone-open-handset-alliance-conference-call

IDC, 2015, Android and iOS squeeze the Competition [referred 24.02.2015]. Available in www format:
http://www.idc.com/getdoc.jsp?containerId=prUS25450615

NIST, 2007, Wireless Network Security for IEEE 802.11a/b/g and Bluetooth (DRAFT) [referred 08.2007]. Available in PDF format:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.6200&rep=rep1&type=pdf

NIST, 2013, Guidelines for Managing the Security of Mobile Devices in the Enterprise [referred 06.2013]. Available in PDF format: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Kaspersky, 2014, Consumer security risks survey 2014: multi-device threats in a multi-device world [referred 06.2014]. Available in PDF format: http://media.kaspersky.com/en/Kaspersky_Lab_Consumer_Security_Risks_Survey_2014_ENG.pdf

Private WiFi, 2014, The Hidden Dangers of Public WiFi [referred 10.2014]. Available in PDF format: http://www.privatewifi.com/wp-content/uploads/2015/01/PWF_whitepaper_v6.pdf

Kaplan, 2012, Google employs Bouncer to cleanse Android malware [referred 05.02.2012]. Available in www format: http://www.itnews.com.au/News/289242,google-employs-bouncer-to-cleanse-android-malware.aspx

Kaspersky, 2015, Perception and knowledge of IT threats: the consumer's point of view [referred 07.03.2015]. Available in PDF format: https://www.kaspersky.com/downloads/pdf/kaspersky-lab_ok-consumer-survey-report_eng_final.pdf

StatCounter Global, 2015, Top 7 Tablet OSs from to Feb to Mar 2015. Available in www format: http://gs.statcounter.com/#tablet-os-ww-monthly-201502-201503-bar

Statista, 2015, Number of available applications in the Google Play Store from December 2009 to February 2015 [referred 26.02.2015]. Available in www format: http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

WatchGuard, 2015, Set the Wireles0stication Method. Available in www format: http://www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html#cshid=en-US/wireless/wireless_auth_method_set_c.html

Wilkins, 2011, WLAN Authentication and Encryption [referred 09.11.2011]. Available in www format:
http://blog.pluralsight.com/wireless-encryption-authentication

Wikipedia, 2015, Wardriving [referred 13.02.2015]. Available in www format:
http://en.wikipedia.org/wiki/Wardriving

Wikipedia, 2015,Wi-Fi Protected Access [referred 26.02.2015]. Available in www format:
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

Wikipedia, 2015, Wired Equivalent Privacy [referred 07.03.2015]. Available in www format:
http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy